



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/832,679	04/10/2001	W. Alexander Hagen	020860-000510US	1877
20350	7590	07/12/2005		
TOWNSEND AND TOWNSEND AND CREW, LLP TWO EMBARCADERO CENTER EIGHTH FLOOR SAN FRANCISCO, CA 94111-3834				EXAMINER MATTIS, JASON E
				ART UNIT 2665 PAPER NUMBER

DATE MAILED: 07/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/832,679	HAGEN, W. ALEXANDER
	Examiner	Art Unit
	Jason E. Mattis	2665

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 12 April 2005.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-61 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-61 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

- Certified copies of the priority documents have been received.
- Certified copies of the priority documents have been received in Application No. _____.
- Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) Notice of Informal Patent Application (PTO-152)

6) Other: _____.

DETAILED ACTION

1. This Office Action is in response to the amendment filed on 4/12/05. Due to the new grounds of rejection, this Office Action is made non-final.

Claim Objections

2. Claims 17, 19, 24, and 49 are objected to because of the following informalities:

Claims 17, 19, 24, and 49 state, "said mobile terminal"; however, there is no prior mention of a mobile terminal in these claims or in claim 1, which these claims depend on. It is recommended that "said mobile terminal" be changed to "said terminal".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-4, 7-15, 19, 23-24, 30-33, 36-42, 44-45, 49, 53-54, and 60 are rejected under 35 U.S.C. 102(e) as being anticipated by Sitaraman et al. (U.S. Pat. 6301618).

With respect to claims 1 and 30, Sitaraman et al. discloses a system and method for providing terminals controlled access to a public network using the public network connection of a private network (**See column 1 line 63 to column 2 line 52 and Figure 1 of Sitaraman et al. for reference to a system and method of granting authorization for a host 12 to connect to the Internet 20, which is a public network**). Sitaraman et al. also discloses a network access point for establishing a network connection with a terminal (**See column 1 line 63 to column 2 line 20 and Figure 1 of Sitaraman et al. for reference to an access point 14, that establishes a connection with a host 12, which is a terminal**). Sitaraman et al. further discloses a network access server (**See column 1 line 63 to column 2 line 20 and Figure 1 of Sitaraman et al. for reference to the access point consisting of a series of network access servers**). Sitaraman et al. also discloses a first network interface between the network access server and the network access point (**See column 1 line 63 to column 2 line 20 and Figure 1 of Sitaraman et al. for reference to the access point consisting of the network access server, meaning since they are made up of the same devices that they must have an interface between them**). Sitaraman et al. further discloses a second network interface between the network access server and the public network connection of the private network (**See Figure 1 of Sitaraman et al. for reference to the access point 14, which consists of the network access server, having an interface to the Internet 20, which is a public network interface of the**

private network). Sitaraman et al. also discloses that the network access server is configured to establish and control a network connection between a terminal having a connection with the access point and the public network through the public network connection of the private network without a connection being established between the terminal and the private network (**See column 2 lines 21-52 and Figure 1 of Sitaraman et al. for reference to the access point 14 establishing a connection between the host 12 and one of the domains, which may be the public Internet 20, without establishing a connection to the other domains, which are the private networks).**

With respect to claims 2-4 and 31-33, Sitaraman et al. discloses that the access point has a wireless network interface and the terminal is a mobile terminal having a wireless network interface for establishing a wireless connection between the access point and the terminal (**See column 1 lines 43-62 of Sitaraman et al. for reference to using wireless remote connections meaning the access point and the host must have wireless network interfaces to establish the wireless remote connections with the host being a mobile terminal).**

With respect to claims 7 and 36, Sitaraman et al. discloses including a third network interface between the network access server and the private network (**See Figure 1 of Sitaraman et al. for reference to the access point 14, which consists of the network access server, having an interface to the private domains 16 and 18, which are private networks).**

With respect to claims 8 and 37, Sitaraman et al. discloses that the network access server is resident in the network access point (**See column 1 line 63 to column 2 line 20 of Sitaraman et al. for reference to the access point 14 consisting the network access server**).

With respect to claims 9 and 38, Sitaraman et al. discloses that the network access server and the network access point are co-resident in a computer (**See column 1 line 63 to column 2 line 20 of Sitaraman et al. for reference to the access point 14 consisting of the network access server, which are embodied as hardware and software, which is a computer**).

With respect to claims 10 and 39, Sitaraman et al. discloses that network access server is resident in a computer and that the computer comprises an interface between the network access server and the private network (**See column 1 line 63 to column 2 line 20 and Figure 1 of Sitaraman et al. for reference to the access point 14 consisting of the network access server, which are embodied as hardware and software, which is a computer and for reference to the interface between the network access server and the private domains 16 and 18**).

With respect to claims 11 and 40, Sitaraman et al. discloses that the network access server is resident in the third network interface (**See column 1 line 63 to column 2 line 20 and Figure 1 of Sitaraman et al. for reference to the interface to the private domains 16 and 18 being part of the access point 14, which consists of the network access server, meaning the network access server and interface to the private domains are a part of the same device**).

With respect to claims 12 and 41, Sitaraman et al. discloses that the third network interface comprises a local area network adaptor (**See Figure 5 of Sitaraman et al. for reference to an access point 113 having an interface comprising a local area network adaptor to LAN 108).**

With respect to claims 13 and 42, Sitaraman et al. discloses software to register terminals and software to limit access to the public network (**See column 2 lines 21-52 and Figure 1 of Sitaraman et al. for reference to the access point 14 registering and authorizing a user to gain access to one of the domains based on a user identification and authorization information).**

With respect to claims 14 and 44, Sitaraman et al. discloses providing facilities to prevent access by terminals to the private network (**See column 2 lines 21-52 and Figure 1 of Sitaraman et al. for reference to a user need to be authorized to gain access to the private domains 16 and 18 meaning there is a facility to prevent access by hosts to the private networks).**

With respect to claims 15 and 45, Sitaraman et al. discloses that the facilities include facilities to configure separate public access and private access subnets (**See column 2 lines 21-52 and Figure 1 of Sitaraman et al. for reference to providing separate access to the domains, both public and private, meaning that there are separate subnets of users accessing the public and private networks).**

With respect to claims 19 and 49, Sitaraman et al. discloses facilities to route data communicated to and from the mobile terminal over to public network (**See column 1 line 63 to column 2 line 52 and Figure 1 of Sitaraman et al. for reference**

to routing data over a connection from the host 12 through the access point 14 to the correct domain, which includes the public Internet 20).

With respect to claims 23 and 53, Sitaraman et al. discloses a database for maintaining selected information concerning registered terminals (**See column 6 lines 12-59 and Figure 5 of Sitaraman et al. for reference to access point 113 containing an AAA server 114 that contains a large bank of stored service profiles connected with individual users).**

With respect to claims 24 and 54, Sitaraman et al. discloses providing telephony service to the mobile terminals (**See column 1 lines 18-62 of Sitaraman et al. for reference to providing telephony service).**

With respect to claim 60, Sitaraman et al. discloses an apparatus for providing mobile terminals controlled access to a public network using the resources of a private network having a network access point for connecting with the mobile terminals and a public network connection for connecting with the public network (**See column 1 line 43 to column 2 line 20 and Figure 1 of Sitaraman et al. for reference to an access point 14 providing access for hosts 12, which are mobile terminals, to the Internet 20, which is a public network, with a network connection to the Internet 20).**

Sitaraman et al. also discloses a network access server having a network interface for making a network connection with the access point and a network connection to the public network (**See column 1 line 63 to column 2 line 20 and Figure 1 of Sitaraman et al. for reference to the access point 14 consisting of a network access server, meaning there is an interface between the network access server and both the**

access point, which it is a part of, and the Internet 20). Sitaraman et al. further discloses that the network access server is operable to control a connection between a terminal and the public network through the public network connection of the private network without permitting a to be established between the terminal and the private network (**See column 2 lines 21-52 and Figure 1 of Sitaraman et al. for reference to the access point 14 establishing a connection between the host 12 and one of the domains, which may be the public Internet 20, without establishing a connection to the other domains, which are the private networks).**

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 25-29, 55-59, and 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sitaraman et al. in view of Lo et al. (U.S. Pat. 6798786).

With respect to claims 25-29 and 55-59, Sitaraman et al. does not disclose an integration operator network with a central database maintaining information about network access servers, registered terminals, and network access and usage policies, managing public network access and usage by the mobile terminal with the network

access and usage policies including one of public network access policy information, bandwidth usage policy information and network traffic priority policy information, with the information about the network access servers including one of provider identification, network configuration information, data encryption information, network usage policy information, and provider accounting information, and with the information about the registered terminals including at least one of authorized user identity, terminal address, terminal security policy, terminal service plan identification, data encryption information, terminal status in network, and network usage accounting information.

With respect to claim 61, Sitaraman et al. discloses a distributed system for providing mobile terminals controlled access to a public network using the public network connections of a plurality of private networks (**See column 1 line 43 to column 2 line 20 and Figures 1 and 5 of Sitaraman et al. for reference to an access point 14 providing access for hosts 12, which are mobile terminals, to the Internet 20, which is a public network, with a network connection to the Internet 20**).

Sitaraman et al. also discloses a plurality of geographically distributed network access points and network access servers with a plurality of network interfaces connecting access points to access servers (**See column 1 line 63 to column 2 line 20 and Figures 1 and 5 of Sitaraman et al. for reference to a plurality of access points 113 consisting of a series of network access servers, which are connected to the access points by interfaces, since they are a part of the access points**). Sitaraman et al. also discloses a plurality of second interfaces connecting the network access server with a public connection of a private network (**See Figure 5 of Sitaraman et al.**

for reference to the access points 113, which consists of the network access server, having an interface to the Internet 106, which is a public network interface of the private network). Sitaraman et al. also discloses that the network access servers are configured to establish and control a network connection between a terminal having a connection with the access point and the public network through the public network connection of the private network (**See column 2 lines 21-52 and Figure 1 of Sitaraman et al. for reference to the access point 14 establishing a connection between the host 12 and one of the domains, which may be the public Internet 20, without establishing a connection to the other domains, which are the private networks).** Sitaraman et al. does not disclose an integration operator network located remotely comprising facilities to form the network access servers into a distributed public network access network.

With respect to claims 25-29, 55-59 and 61, Lo et al., in the field of communications, discloses an integration operator network with a central database maintaining information about network access servers, registered terminals, and network access and usage policies, managing public network access and usage by the mobile terminal with the network access and usage policies including one of public network access policy information, bandwidth usage policy information and network traffic priority policy information, with the information about the network access servers including one of provider identification, network configuration information, data encryption information, network usage policy information, and provider accounting

information, and with the information about the registered terminals including at least one of authorized user identity, terminal address, terminal security policy, terminal service plan identification, data encryption information, terminal status in network, and network usage accounting information (**See column 3 line 39 to column 4 line 40 and Figures 1A and 1B of Lo et al. for reference to a call server network, which is an integration operator network, including a call server 12, policy server 18, and network monitor 19, including storage to store network data pertaining to network usage policies that are used to manage access to a public network 20, while storing information including network access policy information, user network usage information, and terminal gateway, or access point, usage information**). Using a separate network to control and manage access to a public network has the advantage of allowing network access to be controlled and monitored for a plurality of sites at a network that is located in one central location.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Lo et al., to combine the call server network, as suggested by Lo et al., with the system and method of Sitaraman et al., with the motivation being to allow network access to be controlled and monitored for a plurality of sites at a network that is located in one central location.

7. Claims 5-6 and 34-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sitaraman et al. in view of Elsasser (U.S. Pat. 6738641).

With respect to claims 5-6 and 34-35, Sitaraman et al. does not disclose that the network uses Bluetooth protocol or IEEE 802.11X wireless LAN protocol.

With respect to claims 5-6 and 34-35, Elsasser, in the field of communication, discloses using Bluetooth protocol or IEEE 802.11X wireless LAN protocol (**See column 1 lines 36-42 of Elsasser for reference to an access point communicating with mobile client devices using either Bluetooth or IEEE 802.11**). Using Bluetooth protocol or IEEE 802.11X wireless LAN protocol has the advantage of communicating using widely used and accepted wireless communication standards that many devices already employ.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Elsasser, to combine using Bluetooth protocol or IEEE 802.11X wireless LAN protocol, as suggested by Elsasser, with the system and method of Sitaraman et al., with the motivation being to communicate using widely used and accepted wireless communication standards that many devices already employ.

8. Claims 16 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sitaraman et al. in view of Skopp et al. (U.S. Pat. 6256739).

With respect to claims 16 and 46, Sitaraman et al. does not disclose using an IP address filter.

With respect to claims 16 and 46, Skopp et al., in the field of communications, discloses using an IP address filter (**See column 6 lines 15-21 of Skopp et al. for**

reference to an access point using an IP address filter to limit network access).

Using an IP address filter has the advantage of allowing access to a network to be granted or denied to users based on the IP address of the user, such that unauthorized users are not allowed to access a network.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Skopp et al., to combine using an IP address filter, as suggested by Skopp et al., with the system and method of Sitaraman et al., with the motivation being to allow access to a network to be granted or denied to users based on the IP address of the user, such that unauthorized users are not allowed to access a network.

9. Claims 17 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sitaraman et al. in view of Lewis (U.S. Pat. 6526506).

With respect to claims 17 and 47, Sitaraman et al. does not disclose encrypting and decrypting data sent and received by the mobile terminal.

With respect to claims 17 and 47, Lewis, in the field of communications, discloses encrypting and decrypting messages transmitted between an access point and a mobile terminal (**See column 6 line 43 to column 7 line7 of Lewis for reference to using an encrypt key to encrypt and decrypt messages which are transmitted between and access point and a mobile terminal).** Encrypting and decrypting data sent and received by a mobile terminal has the advantage of providing security for a mobile data connection.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Lewis, to combine encrypting and decrypting data sent and received by a mobile terminal, as suggested by Lewis, with the system and method of Sitaraman et al., with the motivation being to provide security for a mobile data connection.

10. Claims 18 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sitaraman et al. in view of Mahany (U.S. Publication US 2004/0042421 A1).

With respect to claims 18 and 48, Sitaraman et al. does not disclose dynamically providing network configuration data to the terminals.

With respect to claims 18 and 48, Mahany, in the field of communications, discloses forwarding configuration updates to units in a wireless system (**See page 5 paragraph 58 of Mahany for reference to forwarding configuration updates**). Dynamically providing network configuration data to terminals has the advantage of making sure that the terminals are constantly updated with current information about network connections.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Mahany, to combine dynamically providing network configuration data to terminals, as suggested by Mahany, with the system and method of Sitaraman et al., with the motivation being to make sure that the terminals are constantly updated with current information about network connections.

11. Claims 20-21 and 50-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sitaraman et al. in view of Vaid et al. (U.S. Pat. 6047322).

With respect to claims 20-21 and 50-52, Sitaraman et al. does not disclose monitoring, recording, and controlling bandwidth usage by the terminals.

With respect to claims 20-21 and 50-51, Vaid et al., in the field of communications, discloses monitoring, recording and controlling bandwidth usage of terminals (**See column 6 line 35 to column 7 line 17 of Vaid et al. for reference to monitoring bandwidth over time and controlling bandwidth usage based on the monitored bandwidth**). Monitoring, recording, and controlling bandwidth usage by the terminals has the advantage of allowing better control of system resources such that each terminal is guaranteed a minimum bandwidth usage allowed while limiting each terminal to a maximum bandwidth usage allowed.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Vaid et al., to combine monitoring, recording and controlling bandwidth usage of terminals, as suggested by Vaid et al., with the system and method of Sitaraman et al., with the motivation being to allow better control of system resources such that each terminal is guaranteed a minimum bandwidth usage allowed while limiting each terminal to a maximum bandwidth usage allowed.

12. Claims 22 and 52 rejected under 35 U.S.C. 103(a) as being unpatentable over Sitaraman et al. in view of Meier (U.S. Pat. 6701361).

With respect to claims 22 and 52, Sitaraman et al. does not disclose providing mobile IP support.

With respect to claims 22 and 52, Meier, in the field of communications, discloses an access point providing mobile IP support (**See column 16 lines 56-65 of Meier for reference to providing support for mobile IP terminals**). Providing mobile IP support has the advantage of communicating using a widely used and accepted wireless communication standard that many devices already employ.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Meier, to combine providing mobile IP support, as suggested by Meier, with the system and method of Sitaraman et al., with the motivation being to communicate using a widely used and accepted wireless communication standard that many devices already employ.

13. Claim 43 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sitaraman et al. in view of Emery et al.

With respect to claim 43, Sitaraman et al. does not disclose automatically registering a terminal when the terminal comes within communication range of the network access point.

With respect to claim 43, Emery et al., in the field of communications, discloses automatically registering a terminal when the terminal comes within communication range of a network access point (**See column 8 line 63 to column 9 line 5 for reference to conducting registration procedures when a wireless terminal comes**

in range of an access point). Automatically registering a terminal when the terminal comes within communication range of a network access point has the advantage of reducing the amount of time to set up a communication channel when a wireless terminal wishes to communicate by performing registration as soon as possible.

It would have been obvious for one of ordinary skill in the art at the time of the invention, when presented with the work of Emery et al., to combine automatically registering a terminal when the terminal comes within communication range of a network access point, as suggested by Emery et al., with the system and method of Sitaraman et al., with the motivation being to reduce the amount of time to set up a communication channel when a wireless terminal wishes to communicate by performing registration as soon as possible.

Response to Arguments

14. Applicant's arguments with respect to claims 1-61 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason E. Mattis whose telephone number is (571) 272-3154. The examiner can normally be reached on M-F 8AM-4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on (571) 272-3155. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jem



HUY D. VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600